

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of)	
)	
Implementation of the)	CC Docket No. 96-115
Telecommunications Act of 1996)	
)	
Telecommunications Carriers' Use of)	
Customer Proprietary Network Information)	
and Other Customer Information)	

To: The Commission

**COMMENTS OF THE CELLULAR TELECOMMUNICATIONS
INDUSTRY ASSOCIATION ON THIRD FURTHER NOTICE
OF PROPOSED RULEMAKING**

Michael Altschul
Senior Vice President, General Counsel

**CELLULAR TELECOMMUNICATIONS
& INTERNET ASSOCIATION**
1250 Connecticut Avenue, N.W.
Suite 800
Washington, D.C. 20036
(202) 785-0081

Dated: October 21, 2002

TABLE OF CONTENTS

	<u>Page</u>
I. THE COMMISSION SHOULD NOT PROHIBIT THE FOREIGN STORAGE OF AND ACCESS TO CPNI	2
A. Section 222 Permits Transfers of CPNI Abroad	2
B. Carriers Store and Access CPNI Abroad in the Ordinary Course of Business	4
C. U.S. Law Currently Provides Jurisdiction Over Information Stored Abroad.....	6
II. CPNI REQUIREMENTS IN THE EVENT OF SALE, MERGER, OR BANKRUPTCY	8
III. CONCLUSION	13

SUMMARY

The Cellular Telecommunications Industry Association (“CTIA”) submits these comments in response to the Third Further Notice of Proposed Rulemaking (FCC 02-214) released on July 25, 2002 (“TFNPRM”). The Federal Communications Commission (“Commission”) sought comment on the proposal to restrict foreign storage of and access to domestic customer proprietary network information or “CPNI” and the need for restrictions on the transfer of CPNI in bankruptcy or sale of assets.

CTIA opposes the request of the Federal Bureau of Investigation (“FBI”) to mandate domestic storage of CPNI. Section 222 does not require it and indeed permits transfer of CPNI, in the United States or otherwise, for purposes of providing telecommunications services. The FBI and other law enforcement agencies, contrary to their assertions, will not be hindered in gaining access to such CPNI under existing law. The record further establishes that such restrictions would impact carrier business operations, negatively affect customers, and increase costs.

CTIA also opposes further CPNI rules and restrictions regarding transfer of CPNI as part of a business transaction such as a merger, sale, acquisition, or in bankruptcy. Such rules are unnecessary because CPNI does not lose its character upon such transfers and the Commission has adequate enforcement powers to protect against improvident disclosures. The Commission cannot anticipate the myriad of business activities in which CPNI transfers may come into play but the law of unintended consequences can be anticipated and avoided.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of)	
)	
Implementation of the)	CC Docket No. 96-115
Telecommunications Act of 1996)	
)	
Telecommunications Carriers' Use of)	
Customer Proprietary Network Information)	
and Other Customer Information)	

To: The Commission

**COMMENTS OF THE CELLULAR TELECOMMUNICATIONS & INTERNET
ASSOCIATION ON THIRD FURTHER NOTICE
OF PROPOSED RULEMAKING**

The Cellular Telecommunications & Internet Association ("CTIA")¹ respectfully submits the following comments in response to the Federal Communications Commission's ("the Commission") Third Report and Order and Third Further Notice of Proposed Rulemaking.² Specifically, CTIA opposes rules prohibiting the foreign storage of customer

¹ CTIA is the international organization of the wireless communications industry for both wireless carriers and manufacturers. Membership in the association covers all Commercial Mobile Radio Service ("CMRS") providers and manufacturers, including cellular, broadband PCS, ESMR, as well as providers and manufacturers of wireless data services and products.

² *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, As Amended*, Third Report and Order and Third

proprietary network information (“CPNI”) and further restrictions on the transfer of CPNI in lawful business transactions.

I. THE COMMISSION SHOULD NOT PROHIBIT THE FOREIGN STORAGE OF AND ACCESS TO CPNI

In its *Ex Parte* letter³ dated July 8, 1997, the FBI requests that CPNI be “exclusively stored in, and accessible solely from within, the U.S.” for national security and ease of access for law enforcement in criminal investigations.⁴ CTIA notes, however, that the FBI’s proposed change contradicts Section 222 of the Communications Act, as amended, which permits carriers to transfer CPNI abroad. Moreover, no such ruling is needed since existing legal authority already permits law enforcement to access such information through U.S.-based carriers regardless of whether the information is stored within the U.S. or outside its borders. Furthermore, while the FBI proposal would provide few, if any benefits, it would significantly impact carrier operations and network architecture. Accordingly, the FBI request should be rejected.

A. Section 222 Permits Transfers of CPNI Abroad

Section 222(c) expressly permits a carrier to “use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the

Further Notice of Proposed Rulemaking, CC Docket Nos. 96-115 and 96-149 (Rel. July 25, 2001) [“*TFNPRM*”].

³ Letter from John F. Lewis, Jr., Federal Bureau of Investigation, to William F. Caton, Acting Secretary, Federal Communications Commission, CC Docket No. 96-115 (filed July 8, 1997) (“FBI’s Letter”).

⁴ *Id.* at 5 (emphasis added).

telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.” Nothing in Section 222 suggests that such use, disclosure or access is or can be confined to the United States.

However, even if foreign storage of and access to CPNI were a problem for law enforcement, Section 222 is not a palliative that allows the overarching response favored by the FBI. Instead, resolution of the problem should be a matter properly left to Congress. It would be an extraordinary action for the Commission to declare domestic access and storage to be a requirement of the 1996 Communications Act when apparently neither the FBI nor Department of Justice believed it to be important enough to ask for it as part of the USA PATRIOT ACT in 2001.⁵ Indeed, CTIA can find no other circumstance where records or information produced by other service providers in any industry have such requirements, including, for example, financial institutions.

The Commission also asked for comment on whether carriers should be required to obtain users’ informed written approval for the storage of or access to CPNI abroad. The question already has been answered by the Commission when it decided that Section 222 does not permit a customer to “restrict a telecommunications carrier from using, disclosing or

⁵ P.L. No. 107-56 at <http://www.epic.org/privacy/terrorism/hr3162.html>.

permitting access to CPNI within the circumstances defined in sections 222(c)(1)(A) and (B).”⁶ The same reasoning and result pertains to foreign storage.

B. Carriers Store and Access CPNI Abroad in the Ordinary Course of Business

When the Commission first sought comment on this issue in its *Further Notice of Proposed Rulemaking*,⁷ numerous carriers noted that their basic day-to-day operations make necessary the ability to store and access CPNI abroad.⁸ Today, as the Commission no doubt knows, globalization of business operations has dramatically increased and many of CTIA’s members outsource customer service, call center and billing functions to places as far as India and as close as Canada. The efficiency of outsourcing comes from the ability to access data from the remote location and to store it locally when necessary to perform the desired functions.

The record also shows that the nature of modern networks makes the FBI’s request impossible: CPNI must often be accessed abroad and stored abroad as part of the basic

⁶ TFNPRM, ¶ 81.

⁷ *Second Report and Order and Further Notice of Proposed Rulemaking*, CC Dkt. 96-115 & 97-149 (released Feb. 26, 1998) (“FNPRM”).

⁸ See Reply Comments of Omnipoint Communications Inc. at 6 (filed April 14, 1998) (“Omnipoint Reply”); Reply Comments of Iridium North America at 2 (filed April 14, 1998) (“Iridium Reply”); AT&T Comments on Further Notice of Proposed Rulemaking at 4 n.6 (filed March 30, 1998) (“AT&T Comments”); Comments of Ameritech on Further Notice of Proposed Rulemaking at 1-2 (filed March 30, 1998) (“Ameritech Comments”); Comments of MCI Telecommunications Corporation at 19 (filed March 30, 1998) (“MCI Comments”); Comments of Omnipoint Communications Inc. at 9 (filed March 31, 1998) (“Omnipoint Comments”).

operation of today's telecommunications networks.⁹ For example, the Global System for Mobile Communication ("GSM") requires remote access and storage to allow users to "roam" internationally. In those cases, users trigger an exchange of CPNI across networks that is necessary to handle the calls. While this process is required by the international standards for GSM, GSM Roaming Agreements ensure by contract that the customer's information will be protected according to the domestic law of the place where the user is roaming.

Continuing with the example, on GSM networks, a subset of a user's CPNI is permanently maintained on what is referred to as the Home Location Register ("HLR"), a mobility database that retains information such as the user's phone number, the phone's locations, and service-related information such as service subscription, service restrictions and other data.¹⁰ When a GSM user roams beyond the domain of its HLR, a Visitor Location Register ("VLR") must authenticate and provide service to the user. As part of the basic operation of the GSM network, foreign VLRs must access the domestically stored CPNI on the user's HLR and a temporary subset of the user's CPNI must be stored on the foreign VLR. Thus, in the process of roaming internationally, a user's CPNI *must* be accessed and stored abroad.

⁹ See Comments of Iridium North America at 6-9 (filed March 30, 1998) ("Iridium Comments"); Omnipoint Reply at 6-7; MCI Comments at 17-19; GTE Comments at 7-8 & n.10 (filed March 30, 1998) ("GTE Comments");

¹⁰ Yin-Bing Lin & Imrich Chlamtac, *Wireless and Mobile Network Architectures* 200 (2001).

The GSM example will be replicated for other technologies as communications services become truly global. This does not mean, as discussed below, that the FBI will not have access to the information. To the contrary, they will, but there would be significant ramifications to network architecture if a rule were crafted that required all access and storage of CPNI to be U.S.-based.

C. U.S. Law Currently Provides Jurisdiction Over Information Stored Abroad

In any event, the FCC need not grant the FBI's request because the FBI already has the ability to access CPNI stored abroad by U.S.-based carriers. In its letter, the FBI asserts that its proposal would thwart efforts by U.S.-based criminals and terrorists to “‘create’ *foreign ‘safe havens’* for the storage of their CPNI” with the help of U.S.-based carriers.¹¹ According to the FBI, such foreign safe havens would keep Domestic Customer CPNI effectively out of the reach of U.S. law entities entirely, or undercut timely and confidential law enforcement access to such information. Applicable law simply does not support such assertions. Carriers regularly go to extraordinary lengths to assist law enforcement within the bounds of the law, and CTIA is not aware of a single instance where law enforcement has been denied timely access to any CPNI of a customer of a U.S.-based carrier regardless of where the customer is located or the CPNI is stored.

This is not surprising because the law establishes the obligation to produce information within an entity's custody or control regardless of where it is stored. For

example, the United States has obtained bank or business records located abroad by serving subpoenas on branches of the bank or business located in the United States, *even where production of the records would violate the foreign country's secrecy laws*.¹² Courts have upheld the use of so-called *Bank of Nova Scotia* subpoenas to compel a bank that does business in the United States to turn over records held by a branch of the same bank in a foreign country, even where production of the records would violate the foreign country's secrecy laws.¹³

The validity and viability of this procedure is confirmed in Title 9 of the Department of Justice's own U.S. Attorneys Manual and nothing limits the power to bank records.¹⁴ Moreover, this principle is recognized as an international norm.¹⁵ Finally, Section 222 itself

¹¹ FBI's Letter at 6.

¹² See *In Re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d 817 (11th Cir.), *cert. denied*, 469 U.S. 1106 (1985).

¹³ *Id.* See also *In Re Grand Jury Proceedings (Bank of Nova Scotia)*, 691 F.2d 1384 (11th Cir. 1982), *cert. denied*, 462 U.S. 1119 (1983); *In Re Grand Jury Subpoena Directed to Marc Rich & Company A.G.*, 707 F.2d 663 (2d Cir.), *cert. denied*, 463 U.S. 1215 (1983).

¹⁴ See United States Attorneys' Manual, Title 9, Criminal Division, *available at* http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/index.html

¹⁵ The Restatement (Third) of the Foreign Relations Law of the United States, which represents legal consensus for its subject matter, states in part in Section 442:

(1)(a) A court or agency in the United States, when authorized by statute or rule of court, may order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States.

already appears to answer the question because it contemplates disclosure to authorized law enforcement agencies “as required by law.”¹⁶

For all of the reasons noted above, the Commission should reject the FBI proposal while acknowledging the cooperation and good faith compliance of telecommunications providers with legitimate law enforcement requests for assistance.

II. CPNI REQUIREMENTS IN THE EVENT OF SALE, MERGER, OR BANKRUPTCY

While CTIA recognizes that the Commission’s interest in this issue is spurred by consolidation in the industry and the bankruptcies of competitive local exchange carriers and other service providers, nothing in the record suggests that disposition of CPNI in any previous transaction was inappropriate or problematic. And nothing suggests that any additional rules are necessary to protect customers or the confidentiality of CPNI.

Several reasons support the conclusion that no new rules are needed. First, there is no factual record to suggest a need for additional rules. Second, the CPNI statute imposes a duty on every carrier to protect the confidentiality of CPNI not only obtained from its own customers, but also that CPNI which is obtained from other carriers as well.¹⁷ In the event of sale or merger of assets from one carrier to another, the character of the CPNI does not change, and the obligations of the receiving carrier under the CPNI rules do not change either. Thus, CPNI will always be protected under the rules and the Commission’s

¹⁶ 47 U.S.C. § 222(c)(1).

enforcement powers are considerable to ensure the confidentiality of CPNI no matter which carrier has possession of it.¹⁸

Moreover, the Commission should be very wary of treating CPNI differently than other personal information in a carrier's possession. Telecommunications service providers increasingly bundle telecommunication and non-telecommunications services such as Internet access, billing on behalf of other merchants, content distribution, etc. For customers who find such packages attractive, by adopting special rules for CPNI the Commission could introduce customer confusion and complicate the orderly treatment of personal information in merger, sale or bankruptcy proceedings since some information would be transferred under one regime while other information would transfer in accordance with other information practices of the service provider.

Indeed, an unintended consequence of establishing special rules governing the transfer of CPNI may be to discourage carriers from providing comprehensive online privacy notices combined with terms and conditions of service due to the Commission's apparent antipathy towards using an online privacy policy as an appropriate vehicle for communicating a carrier's information practices.¹⁹ The Commission should have embraced and encouraged a

¹⁷ 47 U.S.C. § 222(a).

¹⁸ CTIA believes the same is true of a non-carrier successor in interest. CPNI is CPNI regardless of who possesses it and it may only be used or disclosed in accordance with the rules.

¹⁹ Second Order, ¶ 88 ("In particular, we likely would not consider a CPNI notice that was combined with other legal terms and conditions, or other privacy information, to comply with our rules if the customer were deemed to have opted-in or opted-out simply by signing up for service.")

unified and comprehensive presentation of online and offline information practices. A customer's CPNI is no more nor less special than a customer's website activities or financial information. Separate notices distinguished only on the basis of esoteric concepts such as "information services" and "telecommunications services" (even though such services are provided through the same device) are more likely to confuse customers rather than assure them.

The Commission took no notice of existing carrier privacy policies when it adopted its CPNI rules and has never addressed why such online notices coupled with terms and conditions for service were an inadequate means of obtaining customer approval and providing choice. Every major wireless carrier had a privacy policy prominently posted on its Web site at the time the Commission published its rules. Numerous wireless carriers today provide notice to customers regarding business transfers of personal information in those policies.²⁰ There is no reason why such a notice would be inadequate, especially when coupled with further explanation and choices in the customer terms and agreement.

Further, the Commission apparently did not consider industry self-regulation as an alternative to formal rules in regard to CPNI. It is unclear why the Commission felt it more

CTIA understands that a privacy policy and terms and conditions may be used to provide notice and choice so long as acceptance of service is not deemed acceptance of the carrier CPNI practices.

²⁰ See Privacy Statement of AT&T Wireless Services (Business Transfers: Information about our users, including personal information, may be disclosed as part of any merger, acquisition, sale of company assets or transition of service to another provider, as well as in the unlikely event of an insolvency, bankruptcy or receivership in which personal information would be transferred as one of the business assets of the company.) <http://www.attws.com/privacy/>

desirable to pass detailed rules that segmented CPNI from other information without any consideration of less restrictive means of protecting customer information.

No rulemaking can anticipate the myriad of possible business transactions and combinations wherein CPNI would play a legitimate role.²¹ Uncertainty about what constitutes CPNI, how it might be transferred -- and its value, could hinder a beneficial asset sale or merger that otherwise would provide for continued service or some consumer benefit. Due diligence in a merger could be complicated as well. Companies operating under a nondisclosure agreement considering merger could be forced to hold back a valuable asset such as CPNI or to disclose the transaction prematurely to give customers some required notice under the CPNI rules.

Clearly, such rules do nothing to protect CPNI (which typically would be subject to confidentiality provisions in such discussions anyway) and likely do more harm than good or have unintended and unforeseeable consequences. In cases where concerns are raised, the Commission certainly could resort to its enforcement powers to prevent an imprudent transfer or use of CPNI just as other agencies have done when companies have attempted to transfer personal information contrary to promises made to customers.²²

²¹ Indeed, it is not even clear that transfer of CPNI would be necessary or desirable in every case. An acquiring company may only be interested in subscriber list information (name, address, telephone number and primary advertising classification), which would not be governed by the CPNI rules at all.

²² See Federal Trade Commission *In re Toysmart.com* <http://www.ftc.gov/opa/2000/07/toysmart.htm>. Toysmart.com's privacy policy had promised customers that their personal information would *never* be shared with third parties. After filing for

Instead of premature rules,²³ the Commission should address this issue simply by recognizing that CPNI is CPNI and will remain CPNI subject to the CPNI rules regardless of how it is disposed of in any particular transaction. That means that whoever possesses CPNI will be governed by the Commission's rules in using and disclosing such information for marketing purposes, which, after all, is the gravamen of Section 222.

bankruptcy, however, the company offered its customer list for sale as one of its assets. The FTC viewed this subsequent offer for sale as an unfair and deceptive trade practice, in light of the promise made in the company's privacy policy and intervened in the transfer. In crafting a settlement agreement, the FTC was willing to permit Toysmart.com to sell the information only to a qualified buyer, meaning one who was in a related market and who would agree to adhere to Toysmart.com's privacy policy. Ultimately, the bankruptcy court approved the sale of the customer list to one of Toysmart.com's original investors for \$50,000, but only after the investor promised to destroy the list immediately.

²³ Rules may also be premature because Congress currently is considering the treatment of personal information in bankruptcy as part of S. 420, the Bankruptcy Reform Act of 2001. Under S. 420, if the company had disclosed a policy to an individual prohibiting the transfer of personally identifiable information about the individual to unaffiliated third persons, and the policy remains in effect at the time of the bankruptcy filing, the trustee may not sell or lease such personally identifiable information to any person, unless such a sale is consistent with the policy. S. 420 further provides that bankruptcy courts, however, can permit a sale after a hearing and "due consideration of the facts, circumstances and conditions of the sale or lease." The court is also required to appoint an independent third party (the "Consumer Privacy Ombudsman") to provide it with information on the company's privacy policy and the impact the sale would have on customer privacy. The ombudsman can present information of the debtor's privacy policy in effect, potential losses or gains of privacy to consumers if the sale or lease is approved, potential costs or benefits to consumers if the sale or lease is approved, and alternatives which mitigate potential privacy losses or potential costs to consumers.

III. CONCLUSION

For all of the reasons above, CTIA urges the Commission to conclude this rulemaking without further action.

Respectfully submitted,

/s/ Michael Altschul

Michael Altschul
Senior Vice President, General Counsel

**CELLULAR TELECOMMUNICATIONS
& INTERNET ASSOCIATION**
1250 Connecticut Avenue, N.W.
Suite 800
Washington, D.C. 20036
(202) 785-0081

Dated: October 21, 2002